UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/493,984	01/28/2000	Robert S. Eisenbart	18926-003220US	2907

20350 7590 02/27/2004

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
SIMITOSKI, MICHAEL J	

ART UNIT	PAPER NUMBER
2134	15

DATE MAILED: 02/27/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

Office Action Summary	Application No.	Applicant(s)	
	09/493,984	EISENBART ET AL.	
	Examin r	Art Unit	
	Michael J Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover she t with the correspondenc address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 23 January 2004.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-23 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-23 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 28 January 2000 is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

NORMAN M. WRIGHT
PRIMARY EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. The amendment of January 23, 2004 (#14/c) has been received and considered.

2. Claims 1-23 are pending.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1, 3, 6, 8, 11, 12 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,005,938 to Banker et al. (Banker) in view of U.S. Patent 5,005,200 to Fischer in further view of Japanese Patent JP409311854A to Yoneda (machine-translation).

Regarding claims 1, 3, 6, 8, 11 and 13 Banker discloses sending a service instance and an entitlement control message (ECM) to a customer in a distributed network (see col. 1, lines 64-67 and col. 2, lines 1-32). The ECM contains a MAC (signature) of the contents of the ECM (see Fig. 5) and the service instances and ECMs are sent separately over the network to the subscribers (see col. 6, lines 36-44). Banker's system lacks generation of a digital signature over both the ECM and service instance. Fischer teaches that by digitally signing multiple objects together, the objects are verifiable and there is an indication of the relationship between each object and the group (see col. 7, lines 63-67). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to digitally sign both the software object and the rules file in the Banker reference. One of ordinary skill in the art would have been motivated to perform such a modification to maintain verifiability while creating an association between the two, as taught by Fischer (see col. 7, lines 63-67). The combination of Banker and Fischer does not explicitly teach sending a signature separate from the data. However, Yoneda teaches that it can be difficult to remove a signature from a document for verification purposes (Technical Problem, ¶8-10) and this is remedied by creating the signature separately from the document (Means, ¶10-11). Yoneda further teaches that separating the signature and data is beneficial because alteration of the file is detectable (Effect of the invention, ¶46-50). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to send the data and signature separately. One of ordinary skill in the art would have been motivated to perform such a modification because there is no need to remove the signature, making verification easier, from the data and to detect alteration of data, as taught by Yoneda (¶8-11 & ¶46-50).

Regarding claim 12, Banker discloses including dates of validity in the authorization data (see Fig. 2).

5. Claims 2, 4, 9 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Banker in view of Fischer in view of Yoneda as applied to claim 1 above, and in further view of U.S. Patent 6,256,393 to Safadi et al. (Safadi). Banker discloses a system, as modified above, that verifies broadcasted information, but lacks specifically receiving software objects. Safadi teaches a system wherein software objects are verified, then downloaded in response to a need for system cable operators to maintain control of the features and applications that run on set-top terminals (see col. 1, lines 19-27 and col. 2, lines 13-39). Safadi's invention determines if the

software object is authorized to use the set-top terminal resources (see col. 2, lines 43-60) and if the object is not authorized, the object is not executed (see col. 2, lines 61-63). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to expand Banker's system to transmit software objects as well as broadcast information. One of ordinary skill in the art would have been motivated to perform such a modification to satisfy a need for cable operators to maintain set-top terminals, as taught by Safadi (see col. 1, lines 19-27 and col. 2, lines 13-39).

6. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Banker in view of Fischer in further view of Yoneda as applied to claim 1 above, and in further view of U.S. Patent 6,012,144 to Pickett. Banker discloses a system, as modified above, but lacks delaying part of the transmission by a predetermined amount of time. Pickett teaches that by breaking messages into pieces and sending them at different times, intercepting all of the pieces of the message is virtually impossible (see col. 3, lines 1-18). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the Banker system to delay transmission of one of the pieces of information. One of ordinary skill in the art would have been motivated to perform such a modification to render interception of both pieces of information virtually impossible, as taught by Pickett (see col. 3, lines 1-18).

7. Claims 7 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Banker ('938) in view of Fischer in further view of Yoneda as applied to claims 1 and 8 above, and further in view of U.S. Patent 5,247,364 to Banker et al. (Banker ('364)). Banker ('938) discloses a system, as modified above, but lacks sending information over different transmission

pathways. Banker ('364) teaches that unlike in-band transactions, out-of-band subscriber terminals receive data over this channel no matter what the channel the subscriber is tuned to (see col. 1, lines 28-44 and col. 2, lines 55-68). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include authorization information on a different transmission pathway. One of ordinary skill in the art would have been motivated to perform such a modification to gain the benefit of delivery regardless of which channel a subscriber was tuned to, as taught Banker ('364) (see col. 1, lines 28-44 and col. 2, lines 55-68).

8. Claims 14, 15 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Banker ('938) in view of U.S. Patent 5,247,364 to Banker et al. (Banker ('364)) in further view of Yoneda. Banker ('938) discloses a system as modified above, but lacks sending information over different transmission pathways. Banker ('364) teaches that unlike in-band transactions, out-of-band subscriber terminals receive data over this channel no matter what the channel the subscriber is tuned to (see col. 1, lines 28-44 and col. 2, lines 55-68). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include authorization information on a different transmission pathway. One of ordinary skill in the art would have been motivated to perform such a modification to gain the benefit of delivery regardless of which channel a subscriber was tuned to, as taught Banker ('364) (see col. 1, lines 28-44 and col. 2, lines 55-68). As modified, Banker does not explicitly teach sending a signature using a third pathway different from at least the first or second pathway. However, Yoneda teaches that it can be difficult to remove a signature from a document for verification purposes

(Technical Problem, ¶8-10) and this is remedied by creating the signature separately from the document (Means, ¶10-11). Yoneda further teaches that separating the signature and data is beneficial because alteration of the file is detectable (Effect of the invention, ¶46-50). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to send the signature over a third pathway, different from at least the first or second pathway. One of ordinary skill in the art would have been motivated to perform such a modification because there is no need to remove the signature, making verification easier, from the data and to detect alteration of data, as taught by Yoneda (¶8-11 & ¶46-50).

9. Claims 16 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Banker ('938) in view of Banker ('364) in further view of Yoneda as applied to claim 15 above, and further in view of U.S. Patent 6,157,721 to Shear et al. (Shear). Banker discloses a system, as modified above, but lacks using multiple signatures, with multiple signing algorithms, to sign and verify the data. Shear teaches that using several dissimilar digital signature algorithms can reduce vulnerability from algorithm compromise (see ABSTRACT). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a plurality of signatures with different signing algorithms in the authorization message and to use one or more of the signatures to validate the message. One of ordinary skill in the art would have been motivated to perform such a modification to reduce vulnerability from algorithm compromise, as taught by Shear (see ABSTRACT).

10. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Banker ('938) in view of Banker ('364) in further view of Yoneda as applied to claim 14 above, and further in view of U.S. Patent 6,256,393 to Safadi et al. (Safadi). Safadi teaches that using a tiered structure (grouping of programs or services) for access control in a broadcast distribution system reduces bandwidth requirements (col. 4, lines 35-65). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Banker's ('364) design to use tiering. One of ordinary skill in the art would have been motivated to perform such a modification to gain the benefit of reduced bandwidth requirements, as taught by Safadi (col. 4, lines 35-65).

11. Claims 22 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Banker in view of Fischer in further view of Yoneda as applied to claims 1 and 8 above, and further in view of U.S. Patent 6,157,721 to Shear et al. (Shear). Banker discloses a system, as modified above, that uses digital signatures for verification, but uses only one per data. Shear teaches that using several dissimilar digital signature algorithms can reduce vulnerability from algorithm compromise (see ABSTRACT). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a plurality of signatures with different signing algorithms in Banker's data and to use one or more of the signatures to validate the data. One of ordinary skill in the art would have been motivated to perform such a modification to reduce vulnerability from algorithm compromise, as taught by Shear (see ABSTRACT).

Response to Arguments

12. The amendments to the specification and claim 4 to overcome the objection to the specification and rejection of claim 4 under 35 U.S.C. 112 are accepted.

13. Applicant's arguments, see paper 14, filed January 23, 2004, with respect to the rejection(s)of claim(s) 1, 8 & 14 under 35 U.S.C. 103(a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Yoneda, as described above.

14. Regarding "First Missing Limitation", page 12 of arguments, Fischer discloses methods of performing cryptographic operations involving digital signatures. Fischer explicitly teaches a benefit for signing multiple pieces of information with one signature as allowing the pieces of information to be identified (to an entity with the ability to decrypt the signature) (col. 7 lines 63-67). *However, the prior art relied upon in the first office action does not explicitly teach sending the signature over the network separately from at least the first information and the second information.*

15. Regarding "Second Missing Limitation", page 12 of arguments, Banker '938 discloses methods to secure the transmission of digital information, distributed such as from a CATV provider to a set-top box (col. 1 lines 20-35). Banker '364 discloses a head end/provider distributing video programming to subscriber terminals/set-top boxes where multiple transmission pathways are used to overcome shortcomings of prior in-band systems (col. 1 lines 15-45) with hardware to support, *inter alia*, the methods disclosed in Banker '364 (Fig. 2).

In response to applicant's argument that "there is no consideration of authentication issues", the fact that applicant has recognized another advantage which would flow naturally from following the suggestion of the prior art cannot be the basis for patentability when the differences would otherwise be obvious. See *Ex parte Obiaya*, 227 USPQ 58, 60 (Bd. Pat. App. & Inter. 1985).

16. In response to applicant's argument that there is no suggestion to combine the references (pages 12-13 of arguments), the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, Banker '364 describes a CATV system using set top boxes, Banker '938 describes security and cryptographic techniques (including digital signatures) with respect to set top boxes and CATV providers and Fischer describes cryptographic techniques as applicable to digital signatures.

17. Regarding "likelihood of success", page 13 of arguments, the examiner does not suggest the 'brute force' combination of the references, but rather specific elements which are shown, in the reference, to be beneficial. Fischer teaches the benefits of signing multiple pieces of information with one signature. Regardless of the purpose of each piece, the teaching applies to any pieces of digital information. The examiner has suggested that because of this teaching, this element of the claim (generating the signature over first information and second information) is not allowable over prior art. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208

USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). The teachings relied upon are applicable to all the combined inventions, regardless each invention's individual purpose.

Conclusion

18. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. "Application of digital signatures based on public key cryptosystems" by Davies and Price was cited for teaching the linking of all parts of a message in creating a digital signature (pages 9-19) and separating the signature and text (abstract and pages 10-11).

b. U.S. Patent 5,659,616 was cited for teaching separating a signature from a message (and sending separately) to reduce the amount of data needing to be encrypted/decrypted (col. 2 & col. 3).

19. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (703)305-8191. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (703)308-4789.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
Washington, DC 20231

Or faxed to:

(703)746-7239 (for formal communications intended for entry)

Or:

(703)746-7240 (for informal or draft communications, please label "PROPOSED" or "DRAFT")

Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA 22202, Fourth Floor (Receptionist).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-9000.

MJS
February 17, 2004

NORMAN M. WRIGHT
PRIMARY EXAMINER